



FAIRFAX COUNTY  
PUBLIC SCHOOLS

## NOTICE OF AWARD

Department of Financial Services

Office of Procurement Services  
8115 Gatehouse Road, Suite 4400  
Falls Church, Virginia 22042-1203  
Telephone: 571-423-3550

**FEB 29 2016**

CONTRACT TITLE: Distribution Denial of Services (DDoS)

CONTRACT NUMBER(S): 4400006665

NIGP CODE(S): 83883

CONTRACT PERIOD: February 28, 2016 through February 28, 2019

RENEWALS: 3

SOLICITATION NUMBER: RFP 2000001720

CONTRACTOR(S):

Level 3 Communications  
1025 Eldorado Blvd  
Broomfield, CO 80021

SUPPLIER ID(S):

1000032487

Contact: Gary Crocco  
Telephone: 804-298-7205  
Email: gary.crocco@level3.com

TERMS: NET 30

FOB: DESTINATION

PRICES: SEE PRICING SCHEDULE

OPS CONTACT:

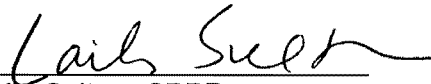
Laila Sultan, CPPB, Contract Administrator  
Phone: (571) 423-3581  
Fax: (571) 423-3550  
E-Mail: lsultan@fcps.edu

B44  
2/29/16

ORDERING INSTRUCTIONS:

Any county department may create a shopping cart into FOCUS (Fairfax County Unified System) indicating the item/service required, the quantity, the payment terms and the delivery date. The shopping cart must be annotated with the contract number.

Requests exceeding the small purchase threshold will be routed to OPS and a purchase order will be executed.

  
\_\_\_\_\_  
Laila Sultan, CPPB  
Contract Administrator

DISTRIBUTION:

FCPS – DIT- Jean Welsh

**PRICE SUMMARY FOR 500 MBS OF CLEAN TRAFFIC (GRE SOLUTION)**

<b>Distributed Denial of Service Attack (DDoS) Protection Services Fees</b>					
<b>Item No.</b>	<b>Item Description</b>	<b>Qty</b>	<b>UOM</b>	<b>Price</b>	<b>Annual Ext.</b>
1.	Professional Services – Site Protection DDoS Detection & Alerting Deployment (non-recurring one-time fee)	2	EA	\$0	\$0
2.	Site Protection – DDoS Detection, Monitoring and Alerting (per Perimeter Router – FCPS has two perimeter routers) (monthly recurring fee)	2	MO	\$1,350	\$16,200
3.	Site Protection – Border Gateway Protocol Redirection (Unlimited) <b>500 MBS of Clean Traffic</b> – Base Bundle (1000 Domains, sixteen /24 Prefix, 1 Location) (monthly recurring fee)	1	MO	\$4,875	\$58,500
4.	Site Protection – Border Gateway Protocol Redirection – Additional /24 Prefix (sixteen /24 prefix totally) (monthly recurring fee)	4	MO	\$0	\$0
5.	Additional Fees (provide specifics of any additional fees, including frequency): _____	—	—	\$0	\$0
	<b>Total Bid (annual fees per year)</b>				<b>\$74,700</b>

**PRICE SUMMARY FOR 1 GIG OF CLEAN TRAFFIC (GRE SOLUTION)**

<b>Distributed Denial of Service Attack (DDoS) Protection Services Fees</b>					
<b>Item No.</b>	<b>Item Description</b>	<b>Qty</b>	<b>UOM</b>	<b>Price</b>	<b>Annual Ext.</b>
1.	Professional Services – Site Protection DDoS Detection & Alerting Deployment (non-recurring one-time fee)	2	EA	\$0	\$0
2.	Site Protection – DDoS Detection and Alerting (per Perimeter Router – FCPS has two perimeter routers) (monthly recurring fee)	2	MO	\$1,350	\$16,200
3.	Site Protection – Border Gateway Protocol Redirection (Unlimited) <b>1 GIG of Clean Traffic</b> – Base Bundle (1000 Domains, sixteen /24 Prefix, 1 Location) (monthly recurring fee)	1	MO	\$6,562.50	\$78,750
4.	Site Protection – Border Gateway Protocol Redirection – Additional /24 Prefix (sixteen /24 prefix) (monthly recurring fee)	4	MO	\$0	\$0
5.	Additional Fees (provide specifics of any additional fees, including frequency): _____ _____	—	—	\$0	\$0
	<b>Total Bid</b> (annual fees per year)				<b>\$94,950</b>

**PRICE SUMMARY FOR 2GIGS OF CLEAN TRAFFIC (DIRECT CONNECT IP CONNECT SOLUTION)**

<b>Distributed Denial of Service Attack (DDoS) Protection Services Fees</b>					
<b>Item No.</b>	<b>Item Description</b>	<b>Qty</b>	<b>UOM</b>	<b>Price</b>	<b>Annual Ext.</b>
1.	Professional Services – Site Protection DDoS Detection & Alerting Deployment (non-recurring one-time fee)	2	EA	\$0	\$0
2.	Site Protection – DDoS Detection and Alerting (per Perimeter Router – FCPS has two perimeter routers) (monthly recurring fee)	2	MO	\$1,350	\$16,200
3.	Site Protection – Border Gateway Protocol Redirection (Unlimited) <b>2 GIGS of Clean Traffic</b> – Base Bundle (1000 Domains, sixteen /24 Prefix, 1 Location) (monthly recurring fee)	1	MO	\$10,500	\$126,000
4.	Site Protection – Border Gateway Protocol Redirection – Additional /24 Prefix (sixteen /24 prefix) (monthly recurring fee)	4	MO	\$0	\$0
5.	Additional Fees (provide specifics of any additional fees, including frequency)  IPVPN Circuit: 3701 FRANCONIA RD ALEXANDRIA, VA 22310  Access: 10 Gig-Ethernet LAN PHY Port: IP VPN Port - 10 GB Usage : \$270/MB ( based on 90th percentile) Install Time: approximately 45 Business days upon receipt of order	1	MO	\$5,500	\$121,000
	<b>Total Bid (annual fees per year)</b>				<b>\$263,200</b>

**PRICE SUMMARY FOR 3 GIGS OF CLEAN TRAFFIC (DIRECT IP CONNECT SOLUTION)**

<b>Distributed Denial of Service Attack (DDoS) Protection Services Fees</b>					
<b>Item No.</b>	<b>Item Description</b>	<b>Qty</b>	<b>UOM</b>	<b>Price</b>	<b>Annual Ext.</b>
1.	Professional Services – Site Protection DDoS Detection & Alerting Deployment (non-recurring one-time fee)	2	EA	\$0	\$0
2.	Site Protection – DDoS Detection and Alerting (per Perimeter Router – FCPS has two perimeter routers) (monthly recurring fee)	2	MO	\$1,350	\$16,200
3.	Site Protection – Border Gateway Protocol Redirection (Unlimited) <b>3 GIGS of Clean Traffic</b> – Base Bundle (1000 Domains, sixteen /24 Prefix, 1 Location) (monthly recurring fee)	1	MO	\$12,450	\$149,400
4.	Site Protection – Border Gateway Protocol Redirection – Additional /24 Prefix (sixteen /24 prefix) (monthly recurring fee)	4	MO	\$0	\$0
5.	Additional Fees (provide specifics of any additional fees, including frequency)  IPVPN Circuit: 3701 FRANCONIA RD ALEXANDRIA, VA 22310  Access: 10 Gig-Ethernet LAN PHY Port: IP VPN Port - 10 GB Usage : \$270/MB ( based on 90th percentile) Install Time: approximately 45 Business days upon receipt of order	1	MO	\$5,500	\$121,000
	<b>Total Bid (annual fees per year)</b>				<b>\$286,600</b>

**PRICE SUMMARY FOR 4 GIGS OF CLEAN TRAFFIC (DIRECT IP CONNECT SOLUTION)**

<b>Distributed Denial of Service Attack (DDoS) Protection Services Fees</b>					
<b>Item No.</b>	<b>Item Description</b>	<b>Qty</b>	<b>UOM</b>	<b>Price</b>	<b>Annual Ext.</b>
1.	Professional Services – Site Protection DDoS Detection & Alerting Deployment (non-recurring one-time fee)	2	EA	\$0	\$0
2.	Site Protection – DDoS Detection and Alerting (per Perimeter Router – FCPS has two perimeter routers) (monthly recurring fee)	2	MO	\$1,350	\$16,200
3.	Site Protection – Border Gateway Protocol Redirection (Unlimited) <b>4 GIGS of Clean Traffic</b> – Base Bundle (1000 Domains, sixteen /24 Prefix, 1 Location) (monthly recurring fee)	1	MO	\$14,550	\$174,600
4.	Site Protection – Border Gateway Protocol Redirection – Additional /24 Prefix (sixteen /24 prefix) (monthly recurring fee)	4	MO	\$0	\$0
5.	Additional Fees (provide specifics of any additional fees, including frequency)  IPVPN Circuit: 3701 FRANCONIA RD ALEXANDRIA, VA 22310  Access: 10 Gig-Ethernet LAN PHY Port: IP VPN Port - 10 GB Usage : \$270/MB ( based on 90th percentile) Install Time: approximately 45 Business days upon receipt of order	1	MO	\$5,500	\$121,000
	<b>Total Bid (annual fees per year)</b>				<b>\$311,800</b>

**PRICE SUMMARY FOR 5 GIGS OF CLEAN TRAFFIC (DIRECT IP CONNECT SOLUTION)**

<b>Item No.</b>	<b>Item Description</b>	<b>Qty</b>	<b>UOM</b>	<b>Price</b>	<b>Annual Ext.</b>
1.	Professional Services – Site Protection DDoS Detection & Alerting Deployment (non-recurring one-time fee)	2	EA	\$0	\$0
2.	Site Protection – DDoS Detection and Alerting (per Perimeter Router – FCPS has two perimeter routers) (monthly recurring fee)	2	MO	\$1,350	\$16,200
3.	Site Protection – Border Gateway Protocol Redirection (Unlimited) <b>5 GIGS of Clean Traffic</b> – Base Bundle (1000 Domains, sixteen /24 Prefix, 1 Location) (monthly recurring fee)	1	MO	\$16,500	\$198,000
4.	Site Protection – Border Gateway Protocol Redirection – Additional /24 Prefix (sixteen /24 prefix) (monthly recurring fee)	4	MO	\$0	\$0
5.	Additional Fees (provide specifics of any additional fees, including frequency)  IPVPN Circuit: 3701 FRANCONIA RD ALEXANDRIA, VA 22310  Access: 10 Gig-Ethernet LAN PHY Port: IP VPN Port - 10 GB Usage : \$270/MB ( based on 90th percentile) Install Time: approximately 45 Business days upon receipt of order	1	MO	\$5,500	\$121,000
	<b>Total Bid (annual fees per year)</b>				<b>\$335,200</b>



**Price Summary for 10 GIGS of clean traffic (Direct IP Connect solution)**

<b>Item No.</b>	<b>Item Description</b>	<b>Qty</b>	<b>UOM</b>	<b>Price</b>	<b>Annual Ext.</b>
1.	Professional Services – Site Protection DDoS Detection & Alerting Deployment (non-recurring one-time fee)	2	EA	\$0	\$0
2.	Site Protection – DDoS Detection and Alerting (per Perimeter Router – FCPS has two perimeter routers) (monthly recurring fee)	2	MO	\$1,350	\$16,200
3.	Site Protection – Border Gateway Protocol Redirection (Unlimited) <b>10 GIGS of Clean Traffic</b> – Base Bundle (1000 Domains, sixteen /24 Prefix, 1 Location) (monthly recurring fee)	1	MO	\$26,400	\$316,800
4.	Site Protection – Border Gateway Protocol Redirection – Additional /24 Prefix (sixteen /24 prefix) (monthly recurring fee)	4	MO	\$0	\$0
5.	Additional Fees (provide specifics of any additional fees, including frequency)  IPVPN Circuit: 3701 FRANCONIA RD ALEXANDRIA, VA 22310  Access: 10 Gig-Ethernet LAN PHY Port: IP VPN Port - 10 GB Usage : \$270/MB ( based on 90th percentile) Install Time: approximately 45 Business days upon receipt of order	1	MO	\$5,500	\$121,000
	<b>Total Bid (annual fees per year)</b>				<b>\$454,000</b>

**SERVICE SCHEDULE**  
**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE**  
(Version Issue Date: February 25, 2015)

1. **Applicability.** This Service Schedule is applicable only where Customer orders Level 3® Distributed Denial of Service Mitigation Service ("Service"). Level 3® Distributed Denial of Service Mitigation Service may be designated as "DDoS", "Denial of Service," "Distributed DoS Service," "DDoS Mitigation Service," or "Distributed DoS Mitigation Service" in Customer Orders, Order acceptance, service delivery, billing and related documents. This Service Schedule incorporates the terms of the Master Service Agreement under which Level 3 provides Services to Customer (the "Agreement"). In the event of any conflict between the Service Schedule and the Agreement, the Service Schedule will govern and control.

2. **Definitions.** Any capitalized terms used herein and not otherwise defined herein shall have the meanings set forth in the Agreement.

**"Always-On"** refers to an option for DDOS Mitigation Direct or DDOS Mitigation Routed GRE Service that continually diverts Customer's inbound internet traffic through the Level 3 Mitigation Infrastructure using BGP networking.

**"Clean (Post-Mitigation) Traffic Capacity"** means the level of traffic using standard DDoS Mitigation Service that is returned to the Customer "clean" following the mitigation process.

**"Distributed Denial of Service Attack" or "Attack"** is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

**"DDoS Mitigation Direct Service" or "Direct Service"** means the DDoS mitigation solution which is implemented using BGP route advertisements as a mechanism to re-route attack traffic through the Level 3 Mitigation Infrastructure. Clean traffic is routed back to the Customer data center over IPVPN/EVPL logical connections between the Mitigation Infrastructure and Customer's border router(s).

**"Level 3 Mitigation Infrastructure" or "Mitigation Infrastructure"** is defined as a collection of Level 3 devices designed to filter malicious attack traffic and pass through legitimate traffic in order to mitigate the potential disruptions caused by a Distributed Denial of Service Attack.

**"Regularly Scheduled Maintenance"** means any scheduled maintenance performed to the Mitigation Infrastructure. Regularly Scheduled Maintenance will not normally result in Service interruption. If Regularly Scheduled Maintenance requires an interruption, Level 3 will: (a) provide Customer seven (7) days' prior written notice, (b) work with Customer to minimize such interruptions and (c) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time where the Mitigation Infrastructure is located on which such maintenance is performed. Emergency maintenance may be performed on less or no notice. Regularly Scheduled Maintenance, emergency maintenance and force majeure events are "Excused Outages".

**"DDoS Mitigation Routed GRE Service" or "Routed GRE Service"** means the DDoS mitigation solution which is implemented using BGP route advertisements as a mechanism to re-route attack traffic through Mitigation Infrastructure. Clean traffic is routed back to the Customer data center using a GRE tunnel.

**"Service Validation"** means the process by which DDoS Mitigation Service is confirmed as available and is required for all Routed GRE Service and Direct Service as a part of the provisioning process (and annually thereafter), enabling Level 3 to obtain a profile of Customer's traffic. Customer will coordinate to schedule such Service Validations when contacted by Level 3 to do so. Service Validation is conducted over (2) windows during which traffic is routed through the Mitigation Infrastructure as follows: (a) an initial 2 hour "test" window, and (b) a 24 hour validation window. Service Validation must be completed for all or a subset of protected Class C subnet prior to routing traffic through the Mitigation Infrastructure. A "Service Validation Acceptance Letter" is provided by Level 3 upon successful completion of this procedure.

**"Special Unavailability"** means unavailability of the DDoS Mitigation Service due to (a) Customer misuse; (b) other negligent or unlawful acts by Customer or Customer Representatives; (c) network unavailability, including telecommunications failures outside of the Mitigation Infrastructure or Level 3 network; (d) problems with Customer's servers or equipment; (e) Customer's traffic load exceeding 10,000,000 TCP (transmission control protocol) packets per-second; (f) any other action or inaction by a third party; or (g) a force majeure event, as defined in the Agreement. Whether Special Unavailability is present shall be determined by Level 3 in its good faith discretion supported by records, data and other evidence.

**"Suspension"** means Level 3's suspension of the DDoS Mitigation Service to Customer: (a) due to a good faith belief by Level 3 that Customer has committed an Abuse as described in Section 9 (Warranty by Customer; Abuses) below; or (b) as otherwise allowed under the Agreement.

3. **Service Description.** The DDoS Mitigation Service is available on Customer's Internet services as described herein. The Customer Order form will specify the type of Mitigation Services and whether those Services are Always-On or On-Demand, as applicable.

Notwithstanding anything in the Agreement to the contrary, Level 3 may, in its sole and absolute discretion, subcontract any or all of the work to be performed under this Service Schedule, including but not limited to, installation, detection, and mitigation services. Services other than the DDoS Mitigation Services provided by Level 3 to Customer that work in conjunction with DDoS Mitigation Services (such as IPVPN Service) are subject to separate Service Schedules.

Direct Service is activated by BGP route advertisement, with logical private line connections over IPVPN/EVPL between the Mitigation Infrastructure and Customer's border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack.

Routed GRE Service is activated by BGP route advertisement and is based upon the GRE protocol with virtual tunnel connections constructed to Customer's border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure, by /24 subnet, enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack.

Routing under either the Direct Service or the Routed GRE Service is asymmetric, with outgoing traffic from Customer to the Internet being forwarded as normal to Customer's Internet Service Provider, without passing through Mitigation Infrastructure.

For On-Demand DDoS Mitigation Services, once the Mitigation Infrastructure is engaged, if an identifiable Attack is not seen by Level 3 within 48 hours then Customer must disengage the traffic re-direction unless otherwise set forth in a Customer Order.

For Always-On DDoS Mitigation Services, the diverted traffic entering Level 3's Mitigation Infrastructure will be inspected and filtered of attack traffic based on predefined filters agreed upon by Level 3 and Customer. Customer must report to Level 3 any new attacks not effectively blocked by predefined filters. Level 3 will respond to new requests for mitigation in accordance with the "Time To Mitigate SLA."

Upon confirmation of an Attack and with the cooperation of Customer, Level 3 shall route Customer's IP traffic to the Mitigation Infrastructure designed to filter malicious Attack traffic and pass through legitimate traffic in order to mitigate the potential disruptions caused by an Attack. However, due to the varying nature of Attacks, Level 3 cannot guarantee that all Attacks will be detected and/or mitigated; nor does Level 3 guarantee that all IP traffic patterns that initially appear to be Attacks are actual Attacks.

Customer must promptly notify Level 3 if it believes it is under Attack and provide Level 3 with reasonable assistance to reroute the IP traffic to the Mitigation Infrastructure in order for the DDoS Mitigation Service to function properly.

A monitoring option for the DDoS Mitigation Service provides more proactive detection of DDoS events by monitoring Customer's routers or Level 3 provider edge routers directly and is available at an additional charge ("Attack Monitoring Services"). Attack Monitoring Services are available only to Customers with management access to their border routers who purchase DDoS Mitigation Services.

Flow Monitoring (FM) Service provides 24x7 monitoring of Customer's border router(s) and alerts for large flood-based Attacks. FM Service requires a reliable feed of netflow sampling and SNMP specific to the Customer's traffic.

Notwithstanding the foregoing, Level 3 reserves the right at any time to: (i) change or supplement the monitoring tools and the mitigation techniques (including but not limited to modifying the Mitigation Infrastructure); (ii) increase or decrease the monitoring tools' sensitivity to anomalous IP traffic patterns; and (iii) modify the definition of anomalous IP traffic patterns that may indicate an Attack.

4. **Charges.** For DDoS Mitigation Services, Customer will be billed monthly in advance based on a fixed rate for mitigation up to a predefined bandwidth level. The manner of billing selected will be set forth in the Customer Order. Fixed rate charges for DDoS Mitigation Service consist of 2 components: (a) a non-recurring installation charge, and (b) a monthly recurring charge ("MRC"). The Service Commencement Date is the first to occur of: (i) Customer's confirmation (which may be via e-mail) that the DDoS Mitigation Service is available following a Service Validation call between Customer and Level 3 and generation of a ticket or (ii) 60 days following submission by Customer of the Order to Level 3.

5. **IP Addresses and Domain Names.** In the event that Level 3 assigns to Customer an IP address as part of the provision of Service, such IP address shall (upon Level 3's request and to the extent permitted by law) revert to Level 3 after termination of the applicable Customer Order for any reason whatsoever, and Customer shall cease using such address. At any time after such termination, Level 3 may re-assign such address to another user. In the event that Level 3 obtains for Customer a domain name (which may be required in some European jurisdictions), Customer shall be the sole owner of such domain name.

With regard to domain names, Customer shall be solely responsible for:

(A) Paying any fees (including renewal fees) relating thereto;

(B) Complying with any legal, technical, administrative, billing or other requirements imposed by the relevant domain name registration authority;

(C) Modifying such domain name in the event Customer changes service providers; and

(D) all third party claims (including claims for intellectual property infringement) relating thereto, and Customer shall indemnify and hold Level 3 harmless from all such claims and expenses (including legal fees and court costs) related thereto.

**6. Bandwidth Overages.** Clean (Post Mitigation) Traffic bandwidth will be calculated using the 95th percentile method. Level 3 shall gather samples of clean traffic usage returned to Customer, both inbound and outbound, at regular intervals. Level 3 shall discard the highest 5% of the samples for each of inbound and outbound traffic, and the next highest sample becomes the 95th percentile value for the data set. If Customer's Clean (Post Mitigation) Traffic calculation exceeds the pre-defined bandwidth level in a month as set forth in a Customer Order in any 2 months within a rolling 12 month period Level 3 may suspend the DDoS Mitigation Service or offer to renegotiate with Customer to an upgraded Service plan (at additional cost to Customer), at Level 3's option.

## **7. Service Levels and Remedies.**

The following Service Levels are not available prior to the completion of initial Service Validation and if repeat Service Validation has not occurred in the previous 12 month period. To receive credits, Customer must immediately notify Level 3 in writing of events, but in no event later than 10 calendar days after the event. Whether an incident constitutes an event for Service credit purposes will be determined by Level 3 in its good faith discretion supported by records, data and other evidence. Credits are only available against the MRC for the affected DDoS Mitigation Service. The Service levels stated in Sections A - D below apply to the mitigation aspect of DDoS Mitigation Service. Customer acknowledges that the Mitigation Infrastructure is a shared platform, and is therefore subject to potential service degradation when other customers on this platform experience DDoS Attacks and/or during maintenance events.

**(A) DDoS Mitigation Service Levels, Service Credits and Chronic Termination Rights.** Level 3 shall use commercially reasonable efforts to make the Level 3 Mitigation Infrastructure available to Customer one hundred percent (100%) of the time once Customer's IP traffic is routed to the Level 3 Mitigation Infrastructure in response to a confirmed Denial of Service Attack until Customer's IP traffic is re-routed back to normal following cessation of such Attack (the "Mitigation SLA"). For purposes of this Mitigation SLA, a "Mitigation Service Outage" means that the Level 3 Mitigation Infrastructure is unavailable to Customer (i.e., the Customer cannot pass traffic through the Level 3 Mitigation Infrastructure) for more than 60 consecutive seconds, except during an Excused Outage, periods of Special Unavailability or periods of Suspension. A Mitigation Service Outage shall only be deemed to have occurred after Customer's IP traffic has begun to route to the Mitigation Infrastructure in response to a confirmed Attack. The duration of the Mitigation Service Outage shall be determined by Level 3 in its good faith discretion using information collected from Level 3 trouble tickets and/or data collected on the Mitigation Infrastructure.

In the event a Mitigation Service Outage lasts 4 or less consecutive hours, upon Customer request Level 3 will provide a service credit to Customer equal to 3 days of the MRC associated with the DDoS Mitigation Service at the affected location (the MRC of the affected location ÷ 30 calendar days x 3).

If a particular Mitigation Service Outage reported by Customer lasts more than 4 consecutive hours, upon Customer request Level 3 will provide a service credit to Customer equal to 5 days of the MRC associated with the DDoS Mitigation Service at the affected location (MRC of the affected location ÷ 30 calendar days x 5).

In no event will Customer receive a credit for more than 1 incident per day pursuant to the terms of this Section 7(A), regardless of the number of times Level 3 fails to comply with the Mitigation SLA during that day.

In addition to Customer being entitled to the above credit(s), as Customer's sole remedy for any non-performance of the Service, the additional termination rights apply:

(a) in the event a Mitigation Service Outage extends for 10 or more consecutive days, Customer shall have the right, for 30 days following the start of such Mitigation Service Outage, to terminate the affected DDoS Mitigation Service under the applicable Order without early termination liability;

(b) in the event of 7 separate occurrences of Mitigation Service Outage each lasting at least 60 minutes in a 90 day period, Customer shall have the right, for 30 days following the 7th such occurrence, to terminate the affected DDoS Mitigation Service under the applicable Order without early termination liability;

(c) if Customer has procured from Level 3 an IPVPN circuit as part of the DDoS Mitigation Service, Customer's termination rights hereunder extend to such IPVPN Service.

**(B) Time to Mitigate Service Level.** Level 3 agrees to deploy mitigation following notice by Customer and Customer properly routing traffic to the Mitigation Infrastructure during an Attack. Level 3 begins mitigating as soon as it begins receiving traffic. The Time to Mitigate value depends on several factors, including (i) the length of time for Customer to properly route traffic; (ii) the length of time it takes for routes to propagate to the Internet at large; and (iii) the type of Attack (see below).

Attack Type	Time to Mitigate Service Level
• UDP/ICMP Floods	10 minutes
• SYN Floods	10 minutes
• TCP Flag Abuses	10 minutes

Mitigation requiring traffic analysis and custom signature development is not covered under the Time to Mitigate Service Level ("TTM SLA"). The remedies for failure to meet the TTM SLA are listed below.

**(C) Consistency of Mitigation Service Level and Remedy for Time to Mitigate Service Levels**

The Time to Mitigate is based from the time that traffic is properly routed through the Level 3 Mitigation Infrastructure, and is further measured based upon the ratio of clean traffic to Attack traffic that is forwarded to Customer after the Time to Mitigate has elapsed ("Consistency of Mitigation"). During any given calendar month, if Level 3 fails to meet the TTM SLA as measured by the Consistency of Mitigation parameters of 95%, the following credits will be issued:

- Single event – less than one (1) hour – in the event that the TTM SLA is exceeded but the mitigation meets the Consistency of Mitigation parameters of 95% within 1 hour, Customer will be entitled to receive a service credit equal to the pro-rated charges for 1 day of the MRC of the affected DDoS Mitigation Service;
- Single event – in the event that the TTM SLA is exceeded and the mitigation does not meet the Consistency of Mitigation parameters of 95% for 1 hour or more, Customer will be entitled to receive a service credit equal to for the pro-rated charges for 2 days of the MRC of the affected DDoS Mitigation Service.
- Single Event lasting more than 6 hours – in the event that the TTM SLA is exceeded – with mitigation not meeting the Consistency of Mitigation parameters of 95% for a period of 6 hours or more, Customer will be credited with 7 days of the MRC of the affected DDoS Mitigation Service.

**(D) Attack Monitoring Services (Flow Based) Service Level**

A credit as set forth below will be provided if an Attack Monitoring Failure to Notify Event occurs. An "Attack Monitoring Failure to Notify Event" or "FTN Event" is an event in which an Attack Monitoring DDoS alert occurs but steps to notify Customer within a period of 15 minutes from the time that Level 3 receives a "Type DDoS" alert are not taken.

For each FTN Event that occurs during a calendar month, Customer will be entitled to receive a service credit equal to the pro-rated charges for 3 days of the MRC applicable to the affected site(s). If 3 or more FTN Events occur during a calendar month, in lieu of service credits, Customer shall have the right, for 30 days following the 3rd FTN Event, to terminate the applicable Service without liability.

**(E) General Terms for all Service Levels**

Credits shall only apply for DDoS Mitigation Service provided pursuant to an MRC, and will not apply to any other DDoS Mitigation Service, including, without limitation, any custom service. Duplicative credits (e.g., for both a Mitigation SLA and a TTM SLA) will not be awarded for a single incident. The aggregate credits under subparts (A), (B), (C) & (D) above to be provided in any calendar month shall not exceed 100% of the MRC of the affected DDoS Mitigation Service. Service Validation must be successfully completed within the previous 12 month period for the TTM SLA and Consistency of Mitigation SLAs to apply for Routed GRE Service and Direct Services. The Service Level credits and termination rights stated in this Service Schedule shall be Customer's sole and exclusive remedies with respect to the DDoS Mitigation Service and related Services provided hereunder.

**8. Customer Responsibilities.** Customer must provide to Level 3 an up-to-date point of contact with 24x7 availability who Level 3 will coordinate with upon detection of an Attack. Customer is solely responsible for updating such point of contact information, as necessary.

Customer must cooperate with Level 3 and Level 3's partners or subcontractors in coordinating setup of the DDoS Mitigation Service, including but not limited to, placing the necessary routing device at the edge of Customer's environment and cooperating with Level 3 in the rerouting of IP traffic to the Level 3 Mitigation Infrastructure during an Attack.

For the Direct Service, Customer must procure from Level 3 connectivity between the Connect Backbone and the Customer Site (border routers) per the following criteria (i) the demarcation point is the physical network port of the Mitigation Infrastructure, (ii) the connectivity must consist of at least 1 IPVPN circuit directly to the port on the Mitigation Infrastructure from each of Customer's data centers; and (iii) any Ethernet circuit must support 802.1Q. Provisioning begins upon confirmation of IPVPN circuit availability. Level 3 may suspend Direct Services if Level 3 determines that any Customer provided equipment is causing interference with the Connect Backbone or other customers. Any IPVPN circuit provided by Level 3 will be subject to service levels as set forth in Level 3's standard service schedule for such service or otherwise agreed in writing by Customer and Level 3.

Customer is required to redirect traffic off of the Level 3 Mitigation Infrastructure within 48 hours of notification that there is no longer any observed Attack traffic.

Customer must promptly notify Level 3 of any events that may cause significant IP traffic pattern changes for the Customer network being monitored through the DDoS Mitigation Service.

Customer must promptly notify Level 3 if it believes it is under an Attack in order for the DDoS Mitigation Service to be activated effectively.

Customer must establish and consistently maintain reasonable and adequate security policies and devices for defense of its assets. Customer acknowledges that DDoS mitigation is regarded as a tool that can be used as part of the Customer's overall security strategy, but not as a total solution.

Customer understands and expressly consents that in the performance of its obligations hereunder, notwithstanding any other requirements in the Agreement between Level 3 and Customer, Level 3 (or its subcontractor) may route Customer traffic to Level 3 Mitigation Infrastructure which is located in a country other than the country of origination and/or destination of such traffic.

In the event Customer or Level 3 determine that the DDoS Mitigation Service is being affected by a continuing error, conflict or trouble report, or similar issue (in each case a "Chronic Problem") caused by the Customer, Customer shall resolve any Chronic Problem by taking whatever steps are deemed necessary to rectify the same, including, but not limited to: (i) removing or modifying the existing DDoS Mitigation Service configuration (or requesting Level 3 to remove the same); or (ii) replacing Customer's equipment providing distributed denial of service Mitigation should that be deemed necessary. If Customer has not remedied the Chronic Problem within 30 days of request by Level 3, then Level 3 may suspend or terminate the DDoS Mitigation Service.

**9. Warranty by Customer; Abuses.** Customer represents and warrants that : (a) in the performance of its obligations and use of the DDoS Mitigation Service by Customer and any Customer representatives, users, employees, subcontractors, agents or any other person under its responsibility (collectively "Customer Representatives"), Customer and Customer Representatives will not violate any applicable laws and/or infringe the intellectual property or privacy rights of any third party; (b) Customer and the Customer Representatives will not use the DDoS Mitigation Service in a manner which constitutes an Abuse (as defined below); (c) the information and other data that Customer transmits and receives in connection with the use of the DDoS Mitigation Service provided hereunder complies and will at all times comply with all applicable laws and do not and will not infringe the intellectual property or privacy rights of any third parties; (d) Customer and Customer Representatives will not knowingly and intentionally transmit, introduce or allow to be introduced, either through it, or any third party over which Customer has control, any virus, worm, "Trojan horse" time bomb or similar contaminating/destructive feature or other malicious code using the DDoS Mitigation Service; and (e) when using the DDoS Mitigation Service (or allowing others to use the DDoS Mitigation Service) Customer and Customer Representatives will comply with all applicable acceptable use policies and will not cause or allow others to cause the disruption of other parties' use or enjoyment of the Internet.

Without limiting the foregoing, the following shall be deemed impermissible uses of the DDoS Mitigation Service ("Abuses") and each shall constitute a material breach by Customer of this Service Schedule and applicable Agreement:

(a) causing, aiding, encouraging, or facilitating a domain or URL hosted by Level 3 for Customer or any Customer Representative to point to or otherwise direct traffic to any material that violates any applicable law or regulation;

(b) using or facilitating the use of the DDoS Mitigation Service to (including by pointing to web sites or locations that): create, transmit, distribute or store material that include tools designed for compromising security (including but not limited to password guessing programs, cracking tools or network probing tools); violate U.S. and any other applicable export control, data protection or anti-terrorism laws; impair the privacy of communications; knowingly contain viruses; and/or

(c) violating Level 3's then-current acceptable use and privacy policies located at [www.level3.com](http://www.level3.com).

Notwithstanding anything to the contrary in the Agreement, Customer, at its own expense, shall indemnify, defend, and hold harmless Level 3 and its directors, officers, trustees, shareholders, employees, independent contractors, subsidiaries, Affiliates, agents, successors and assigns from and against any and all losses, costs, liabilities, judgments, damages (whether direct, indirect or consequential) and expenses, including, without limitation, reasonable attorneys' fees and expenses arising out of or relating to any claim, action, allegation, investigation, proceeding or suit concerning any: (i) conduct by Customer which constitutes an Abuse; (ii) third-party claim arising from or relating to any content provided or delivered by or for Customer or Customer Representative in connection with the DDoS Mitigation Service; (c) content provided or delivered by or for Customer or Customer Representatives in connection with the DDoS Mitigation Service, and/or (d) breach of Customer's warranties, representations, or obligations set forth in this Section 9.

**10. Restrictions.** If Level 3 provides Customer with portal access in connection with the DDoS Mitigation Service, Customer will use such access solely as for use with the DDoS Mitigation Service in accordance with this Service Schedule and the Agreement, and Customer will be responsible for any unauthorized access to or use thereof. Level 3 reserves the right to adhere to the safe harbor provisions of the Digital Millennium Copyright Act and any other equivalent legislation in any country or jurisdiction. For the avoidance of doubt and without prejudice of the foregoing, Level 3 reserves the right to (i) apply the limitations or exclusions of liability of the aforementioned laws and regulations and any applicable copyright laws; and (ii) suspend the Services or pull down Customer's data or content that is allegedly infringing any third party rights (in accordance with a third party complaint). Customer understands and acknowledges that the DDoS Mitigation Service is not suitable for the maintenance, receipt or transmission of protected health information consistent with the Health Insurance Portability and Accountability Act (HIPAA), as amended or any other applicable laws in the matter.

**11. Disclaimer.** Notwithstanding anything to the contrary in the Agreement, except as expressly set forth herein, in no event shall Level 3 be liable for any loss or damage (whether direct, indirect or consequential) arising out of or in connection with this Service Schedule.

The DDoS Mitigation Service is provided on an "as is" and "as available" basis, and any and all warranties, representations or conditions, whether express or implied (by contract, statute or otherwise) are excluded to the fullest extent permitted by law. Notwithstanding any language in the Agreement to the contrary, Level 3 shall not be obligated to provide any defense, indemnity or hold harmless obligations with regard to any actual or alleged claim, liability, damage, expense or fees arising in connection with Customer's use of the DDoS Mitigation Service (or any associated software or Services) or otherwise arising in connection with this Service Schedule.

## **12. Additional Terms and Conditions Associated with the Service.**

Level 3 may terminate any Customer Order in the event that Level 3 cannot maintain any required regulatory approvals, despite its reasonable efforts to do so. Level 3 may temporarily suspend any DDoS Mitigation Service immediately in the event Level 3 has a good faith belief that such suspension is reasonably necessary to mitigate damage or liability that may result from Customer's continued use of the DDoS Mitigation Service. In the event of any expiration or termination of any Service, Customer's access to the applicable Services will end and Level 3 will not be responsible for assisting Customer with any transition to an alternative provider, notwithstanding anything to the contrary in the Agreement.

All right, title and interest in and to the DDoS Mitigation Service, the Mitigation Infrastructure, Level 3 network or any other technology utilized by Level 3 to deliver the DDoS Mitigation Service, and all related technology, computer code, and other related materials and results thereof (including the domain name server, proxy system, routing, switching, IP network, software, data and know-how), and all intellectual property embodied therein or derived therefrom (the "Proprietary Materials") shall be the sole and exclusive property of Level 3, its Affiliates and/or its licensor(s), and nothing in this Service Schedule or the Agreement shall be construed to convey to Customer any right, title, license or interest in or to such Proprietary Materials. Neither Customer, nor anyone acting on behalf of Customer may reverse engineer, decompile, modify or create derivative works of any of the Proprietary Materials. Level 3 and its licensors reserves for themselves all rights not granted herein. Nothing in this Service Schedule or the Agreement grants Customer any rights to, and Customer is expressly prohibited from, reselling the DDoS Mitigation Service or using any component of the DDoS Mitigation Service or Proprietary Materials to create or offer derivative versions of the DDoS Mitigation Service either directly, or through a third party, as a standalone service offering, as bundled with Customer's services or products, or on a service-bureau basis.

UNDER NO CIRCUMSTANCES SHALL EITHER PARTY BE LIABLE TO THE OTHER OR TO ANY THIRD PARTIES FOR INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING LOST PROFITS, LOSS OF USE OF EQUIPMENT OR SERVICES, OR DAMAGES TO BUSINESS OR REPUTATION ARISING FROM THE PERFORMANCE OR NON-PERFORMANCE OF ANY ASPECT OF THIS AGREEMENT WHETHER IN CONTRACT OR TORT OR OTHERWISE, AND WITHOUT REGARD TO WHETHER OR NOT NOTICE OR ADVICE OF THE POSSIBILITY OF SUCH DAMAGES HAS BEEN GIVEN; PROVIDED HOWEVER THE FOREGOING SHALL NOT APPLY OR OTHERWISE LIMIT CUSTOMER'S OBLIGATIONS TO INDEMNIFY LEVEL 3 SET FORTH IN SECTION 9. CUSTOMER RECOGNIZES THAT THE INTERNET CONSISTS OF MULTIPLE PARTICIPATING NETWORKS THAT ARE SEPARATELY OWNED AND THEREFORE ARE NOT SUBJECT TO THE CONTROL OF LEVEL 3. MALFUNCTION OR CESSATION OF INTERNET SERVICES BY INTERNET SERVICE PROVIDERS OR OF ANY OF THE NETWORKS THAT FORM THE INTERNET MAY MAKE THE SERVICES TEMPORARILY OR PERMANENTLY UNAVAILABLE. OCCASIONAL TEMPORARY INTERRUPTIONS OF SERVICES MAY OCCUR FROM TIME TO TIME. CUSTOMER AGREES THAT LEVEL 3 SHALL NOT BE LIABLE FOR DAMAGES INCURRED OR SUMS PAID WHEN THE SERVICES ARE TEMPORARILY OR PERMANENTLY UNAVAILABLE, INCLUDING DUE TO MALFUNCTION OR CESSATION OF INTERNET SERVICES BY NETWORK(S) OR INTERNET SERVICE PROVIDERS NOT SUBJECT TO THE CONTROL OF LEVEL 3, OR DUE TO ANY ACCIDENT OR ABUSE BY CUSTOMER. THE INTERNET IS NOT A SECURE NETWORK; CONFIDENTIAL OR SENSITIVE INFORMATION SHOULD NOT BE TRANSMITTED OVER THE INTERNET OR STORED ON COMPUTERS DIRECTLY CONNECTED TO THE INTERNET.

[Remainder of page intentionally blank]